Polk State College Information Security Guidelines

Polk State College has established standards for the protection and security of information, and for the use of information and technology resources. The goal of Polk State's standards are to ensure that information integrity is maintained, its availability is ensured, its confidentiality is preserved, and its access is controlled. Security guidelines protect information from unauthorized viewing, modification, dissemination, or destruction and provide recovery mechanisms from accidental loss. The security of information is the responsibility of all people who are authorized to access it. All employees are expected to abide by these standards and will be required to sign a statement affirming that they have read, that they understand, and that they intend to comply with the provisions stated herein, prior to obtaining access to the organization's data systems and networks. Any intent to do harm to the College equipment or information will result in personnel and civil action as deemed appropriate.

The protection of faculty, student, and staff confidentiality and employee privacy, in accordance with applicable laws and our personnel and student information release policies, is of utmost importance. The Information Technology Advisory Group (ITAG) is responsible for establishing and maintaining the organizational technology services handbook of guidelines, forms and standard operating procedures. The focus of these activities is on information, regardless of the form it takes, the technology used to manage it, where it resides, and which people possess it or have access to it.

The information security guidelines apply to employees, customers, volunteers, vendors, contractors, Board members, affiliates and any others who have access to and use Polk State College information resources. The guidelines also apply equally to any information of the organization, including but not limited to electronic data, written or printed information and any other intellectual property of the organization. The information resources include hardware, software, manuals and office equipment. All individuals agree not to disclose information improperly or to use information improperly or unethically for personal or professional gain; or subversive purposes.

I - Critical Business Function

- Reliable technology support services are necessary for the sustained, stable, and consistent institutional, instructional, and infrastructure technology performance to support the many essential activities of Polk State College. A security breach within any of the Polk State College information systems would result in serious consequences, including but not limited to legal liability and degraded reputation. Accordingly, information and system security is a critical component of the business environment and preventative action essential to the reduction of cost and risk over time.

- Information is no longer the exclusive domain of Technology Services - information security is a team effort requiring the participation of every employee who comes in contact with Polk State College and its technology services.

- Every user must understand the College guidelines regarding information security, and must agree in writing to perform his or her work as outlined in the acceptable use guidelines.

II – Information Security Responsibilities and Processes

- Administrators in units and departments will be designated as the Owners of the information used for regular business activities. Information Owners do not legally own the information in question; they are instead members of the Polk State College administrative team who make decisions on behalf of the organization. Information Owners, or their delegates, are required to make the following decisions and perform the following activities:

  a) Approve information-oriented user access control privileges for specific job roles

  b) Approve information-oriented access control requests, which do not fall within the purview of existing job roles

  c) Select a data retention period and schedule for information based on College guidelines, State, and Federal guidelines. Technology Services will implement purge/archiving based on the retention guidelines specified and storage capacity.

  d) Designate a system-of-record (original source) for information from which all administration reports will be derived.

  e) Select special controls needed to protect information (such as additional input validation checks or more frequent back-up procedures).

  f) Define acceptable limits on the quality of their information (accuracy, timeliness, time from capture to usage, etc.).

  g) Approve all new and different uses of their information for tasks such as reporting and cataloging.

  h) Approve all new or substantially enhanced application systems that use their information before these systems are moved into operational status.

  i) Review reports about system intrusions and other events relevant to their information.

  j) Review reports that indicate job roles and specific users that currently have access to that information and correct any identified anomalies.

  k) Select a sensitivity classification category relevant to their information and review this classification periodically for possible downgrading/upgrading.

l) Select a criticality category relevant to their information so that appropriate contingency planning can be performed.

m) Define standard operating procedures to assure information is being stored and handled in accordance with all relevant laws, regulations, and applicable professional standards.

- Information Owners must designate a back-up person to act when unavailable. Owners may not delegate ownership responsibilities to third party organizations such as outsourcing firms or consultants or to any individual who is not a full-time employee. When both the Owner and the back-up Owner are unavailable, the Chief Information Officer (CIO) may make decisions on behalf of the Owner.

III - Information Owners at Polk State College

• Student Data	Director Student Enrollment Services/Registrar
• Learning Systems Data	Director, Instructional Technology
• Financial Data	Controller
• Financial Aid Data	Director of Student Financial Services
• Facilities Data	Director of Facilities
• HR Data	Director of Human Resources
• Security Data	Chief Information Officer
• Foundation Data	Director of Finance, Foundation
• Website Data	Associate VP, Office of Communication and Public Affairs

IV – Supervisors

- Owners do not approve ordinary access control requests. Instead, a user's immediate supervisor approves a request for system access based on existing job roles. If a profile doesn't exist, the supervisor's responsibility is to create the profile, obtain the approval of relevant Owners, and inform Technology Services.

- Similarly, when an employee voluntarily leaves or is terminated by Polk State College, the employee's immediate supervisor is responsible for promptly informing Human Resources who will work with Technology Services to revoke the system and network access privileges concomitant with the employee's user-ID. The supervisor is responsible for communicating with Technology Services regarding the forwarding, automatic messaging, and distribution of content associated with the discontinued account.

- User-ID's are specific to individuals, and must not be reassigned to, or used by, others. Supervisory consequences are required in the case that this behavior is identified.

V – Information Custodians

- Custodians are in physical or logical possession of information and/or Technology Services. Like Owners, Custodians are specifically designated for different types of information. In most cases, Technology Services will act as the Custodian. If a Custodian is not clear based on existing Technology Services operational arrangements, the CIO will designate a Custodian. Custodians follow the instructions of Owners, operate systems on behalf of Owners, but also serve Users authorized by Owners.

- In cases in which the information being stored is paper-based, and not electronic, the Information Custodian responsibilities will logically fall to the department gathering the information. For such systems, Technology Services can offer guidance and suggestions, but will not provide the custodial services.

- Custodians must define the technical options, such information criticality categories, and then allow Owners to select the appropriate options for their information. Custodians also define Technology Services architectures and provide technical consulting assistance to Owners so that technology services can be designed and operated to best meet business objectives. If requested, Custodians additionally provide reports to Owners about information system operations and information security problems. Custodians are furthermore responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and testing information contingency plans.

VI - Information Users:

- Users are not specifically designated, but are broadly defined as any employee with access to internal information or data. Users are required to abide by all security requirements defined by Owners, implemented by custodians, and/or established by Technology Services.

- Users are required to familiarize themselves with, and act in accordance with all Polk State College information security requirements.

- Users are also required to participate in information security training and awareness efforts.

- Users must request access from their immediate supervisor, and report all suspicious activity and security problems.

VII - Information Security:

- Technology Services (and, more particularly, the CIO) is the central point of contact for all information security matters at Polk State College. Acting as internal technical consultants, this Department's responsibility is to create workable information security compromises that take into consideration the needs of various Users, Custodians, and Owners. Reflecting these compromises, this Department defines information security standards, guidelines, and processes applicable to the entire organization. Technology

Services is responsible for: handling all access to control management activities, monitoring the security of Polk State College Technology Services, and collaborating with Human Resources to provide information security training and awareness programs to Polk State College employees. The department is additionally responsible for periodically providing administration with reports about the current state of information security.

- Technology Services must also provide technical consulting assistance related to emergency response procedures and disaster recovery. Guidance, direction, and authority for information security activities are centralized for the entire organization in Technology Services.

- Technology Services is responsible for organizing a computer emergency response team (CSIRT) to promptly respond to virus infection, hacker break-ins, system outages, and similar security problems.

- Technology Services must provide the direction and technical expertise to ensure that Polk State College information is properly protected. This includes consideration of the confidentiality, integrity, and availability of both information and systems. The Department will act as a liaison on information security matters between all departments, and must be the focal point for all information security activities throughout the organization. The Department must perform technology systems risk assessments, prepare action plans, evaluate vendor products, assist with control implementations, investigate information security breaches, and perform other activities that are necessary to assure a secure information-handling environment.

- Technology Services has the authority to create, and periodically modify, both technical standards and standard operating procedures (SOP), which support the information security guidelines outlined in this document. These SOP, when approved by appropriate Polk State College administrators, have the same scope and authority as if they were included in this guideline document.

VIII - Reporting Security Incidents:

- If a user suspects a security incident (such as a virus, spam or unauthorized use of their user-id and password, the incident should be reported to the CIO as the Chief Security Officer.

- Attempted breaches of information are logged and analyzed for patterns of risk assessment purposes.

- The CIO will gather a team of Technology Services employees to investigate the reported security incident, and appropriate forensic external support, to report back to the Information Technology Advisory Group (ITAG) and President's Staff. In certain cases, security incidents may be reported to the appropriate law enforcement agency for prosecution.

Technology Services Responsibilities, Policies and Standard Operating Procedures

Technology Services must establish and maintain sufficient preventive and detective security measures to ensure that Polk State College information is free from significant risk of undetected alteration.

IX – Technology Services Information Security Guidelines Document

- Technology Services is responsible for developing and maintaining this information security guidelines document under the oversight of ITAG.
- The information in this document will be reviewed and evaluated on a regular basis.
- Administration fully supports the development and enforcement of these information security guidelines.

X - Information Security Organization

- The CIO oversees and ensures compliance with technology guidelines and handbook within the organization.
- Technology Services will occasionally test users, inclusive with immediate remediation, to ensure that consistent compliance exists across the organization.
- Third Party connection access requirements to the computer network are documented in contracts and agreements.
- Information security requirements are fully specified in outsourcing contracts.

XI - Asset Classification

- A formal Information Management System (IMS) is in place that tracks the movement of IT assets.
- The IMS is detailed and covers the movement of hardware assets.
- Sensitive information assets are classified as Confidential.
- Classified information transmitted over insecure networks, such as the Internet, must be adequately encrypted.

XII - Personnel Security

- All Polk State College employees receive a pre-employment criminal background check.

- Information security awareness is recognized as a significant risk administration issue. New employees receive information security policies as part of their orientation, and as part of ongoing communication activities.

- Personnel found to be involved in information security breaches are subject to formal disciplinary procedures and appropriate civil action per Florida Statutes, Computer Abuse and Data Recovery Act, 668.801-668.805.

XIII - Physical Security of Technology/Computer Equipment

- There are cipher or magnetic card locks on computer room doors, and codes / authorized cards are limited to authorized persons.

- Computer rooms have installed fire suppression equipment.

- All district computer systems (including phone and communication rooms housed separately from the main data center) are tied into the Uninterrupted Power Supply (UPS) system and a backup generator.

- Computers are checked for sensitive information prior to disposal through a DOD 3 wipe technique OR total destruction of the hard drive.

- Communications closets are locked. Only facilities and networking personnel have key access.

XIV - Computer and Network Security

- There is a documented change control process. Changes to most networks, operating systems or application systems (both legacy and client-server or web) are documented and approved within the request for change within the Technology Services ticket management application.

- Virus detection software is installed on all file servers and personal computers. Virus signature updates are routinely applied. There are adequate preventative controls. Users have been instructed to utilize caution in accessing files, mail attachments and downloads of uncertain origin.

- Backups of production data are performed daily.

- Appropriate, frequent backups of business systems are stored in remote location. Thorough testing of backups occur to validate data recovery and technology services will keep a consistent backup schedule that can referenced as documentation.

- Operations staff maintain a work log (system start and finish times, system errors and corrective actions, confirmation of input and output). Systems are monitored for concerns, with critical systems given more attention.

- There are basic logs/lists of tapes to help trace or locate a backup tape. Media is physically secured and housed in locked rooms or cabinets.

- A network monitoring package and firewalls are in place. Firewall configurations are based upon industry best practices. Operating system and router settings are benchmarked on industry best practices, and kept up-to-date with patches/upgrades recommended by product vendors and/or other professional sources.

- Only the Network Engineer and/or the Network Support Specialists will modify and/or change any network device configuration. Prior to making any changes to a network device, the change will need to be approved by the Manager of Computing Systems and the CIO.

XV - System Access Control

- A formal system access request process exists. An electronic or paper form must be completed in order to create, modify, or delete any user account. Approvals are required and integrated into the Human Resources onboarding processes.

- All users are made aware of their responsibilities with respect to the selection and use of strong passwords with complexity. Passwords expire at every 60 days. Stricter controls exist on sensitive systems or accounts. There are no shared or guest accounts.

- Only authorized users are able to gain access to networked systems from a remote location. There are adequate controls over the authentication of remote users. Access from remote locations is granted through the use of a VPN. Access via VPN is granted to those who complete a form signed by their budget head and appropriate Vice-President. Network access is generally controlled through the use of firewalls at major access points.

- Unique user IDs (with names that do not indicate privileged users) and strong passwords are the rule in order to gain access at the operating system level on all systems. Logon credentials are secure and difficult to guess. There are no anonymous or shared accounts.

- Event logs are kept automatically for most systems showing unauthorized access attempts, privileged operations, major system events, and system failures. Logs are reviewed daily and in response to problems. Logs from sensitive systems are taken offline and stored securely.

- Unsecured wireless networks (which do not require a user id and password) provide internet access only for college faculty, staff and visitors and are separated from the college's network and cannot access any sensitive college information.

XVI - System Development and Maintenance

- Polk State College uses software [*Integrow*] developed and provided by the *Higher Education Technology Group* [HETGroup]. The *Integrow* software (named *Genesis* by Polk State College*)* was developed specifically to address the needs for Florida colleges' unique reporting requirements. Polk State College runs the software with few baseline modifications. Modifications to the baseline software that are necessary to accommodate business rules specific to Polk State College are approved by the users through a formal change control process, and implemented by in-house programming staff and/or vetted consultants.

- Formal College guidelines have been established regarding the steps needed to update or upgrade Operating Systems and User Applications. System administrators, information owners, and network management are involved in testing before any migration from test to production systems is permitted.

- Vendor supplied packages are not modified unless the benefits of doing so are documented and substantial approval from administration has been acquired.

XVII - Application Security

- For purchased applications, the appropriate user is in charge of security of those systems, but will work with technology services on the procurement, implementation, maintenance, and sustained funding/support.

For the Genesis application, security is handled in the following manner:

- A UNIX account is setup by the Lead Computer Operator or delegated to a Computer Operator.

- A Natural account is setup by the Manager of Systems and Programming.

- Application security is granted by the appropriate user security administrator upon review of the user's job requirements.

XVIII - Business Continuity Plan

- The College has a general disaster recovery plan.

- In the event that the production server cannot function due to a disaster, the college purchased a development/disaster recovery server that will be located in an offsite data to continue to service the college community. Additional ERP system backup is available in a separate secure location in the case that the secondary systems that are in place are insufficient.

- A disaster recovery plan exists that includes the necessary steps to facilitate use of the disaster recovery servers in the event of an emergency and the appropriate tasks that are required to maintain business operations and access to information.

- Technology continuity is included in the general Polk State College Continuity of Operations Plan, which is developed and maintained by the Risk Management Department.

XIX – Compliance

- Users who break or violate local, state, and federal laws or contractual obligations will incur supervisory discipline, potential termination, and possible prosecution.

- All managers and staff are educated about their responsibilities through orientation, access to the technology services handbook, and other awareness methods (e.g., newsletters, posters, flyers, etc.). Staff must demonstrate active compliance with information security controls, and must re-affirm their understanding of policies by annual training, acknowledgment and review.

- Standards for secure configuration settings are comprehensive and regularly updated. A comprehensive program of regular reviews of compliance with secure configuration standards is scheduled, aided by automated technical security auditing tools.